中信國際電訊CPC
CITIC TELECOM CPC

TrustCSI™ ATP 進階威脅防護方案

憑藉卓越協同效益，TrustCSI™ ATP能確保企業信息安全

進階網絡威脅及攻擊種類廣泛，數量愈趨增加，令現今企業面對前所未有的高風險困境。**TrustCSI™ ATP**進階威脅防護方案的整合協同效益，為企業全面抵禦對端點、網絡及伺服器(例如檔案、電郵及網頁伺服器)的進階持續性威脅(Advanced Persistent Threat)。這個由中信國際電訊CPC提供的託管式防護方案，令企業盡享24 x 7世界級信息安全優勢，節省成本，免卻繁複管理。

產品特點

- 一站式全面安全管理服務，快速有效地提供進階威脅防護。
- 透過實時監控、主動式威脅通知及消除，全面應對跨基礎架構層上的各類威脅。
- 主動偵測及阻截能避過一般信息安全方案的新型威脅與未知攻擊。
- 各個安全模組積極協作及連繫，共同架構實時信息安全防禦。
- 無間斷運作的分層安全保護系統，包括統一威脅管理(UTM)、網絡應用防火牆(WAF)、電子郵件安全設備(SEG)、沙盒及全天候的託管式安全服務(MSS)。

你最可信賴的信息技術方案伙伴

TrustCSI™ ATP 進階威脅防護方案

TrustCSI™ATP進階威脅防護方案的多重防禦系統，加上中信國際電訊CPC世界級的信息安全基建資源及專業服務，令它成為保障企業信息安全的不二之選。全面的一站式解決方案將全方位保護企業，抵禦網絡各類先進攻擊。

競爭優勢

度身訂製的總體安全方案

TrustCSI™ATP進階威脅防護方案可根據您獨有的基建、資源及需求度身訂製，助您作出適當部署。

互動制式發揮強大聯防效果

不同防禦制式環環相扣，無縫監察於檔案、電郵、網絡流量及網絡應用各大層面的可疑活動。沙盒會即時更新病毒特徵庫，並與UTM、WAF及SEG模組緊密互動，確保用戶安全。

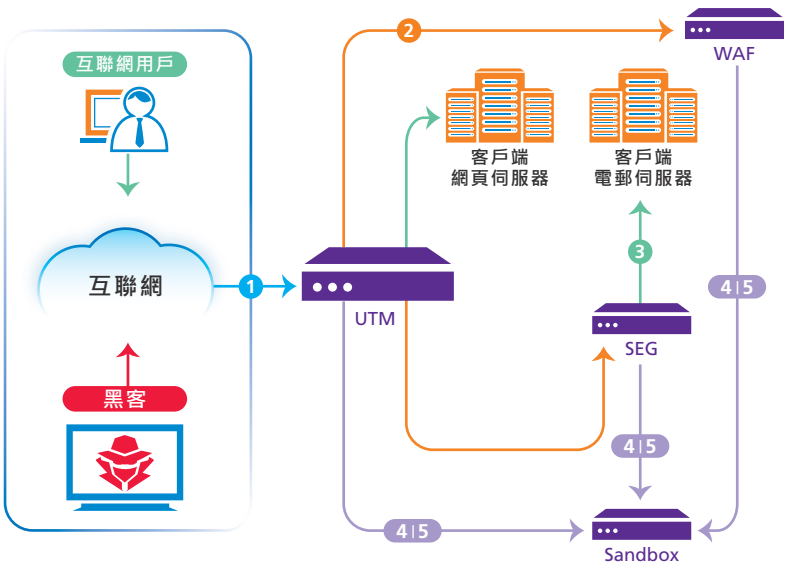
24 x 7的監控及安全通報

安全專家將全天候監控您的企業安全狀況，就系統任何異常發出預警，並提供專業建議以作補救行動。

深入透析安全威脅趨勢

安全運作中心的安全智能平台會分析您的系統漏洞及最新威脅情報，並提供UTM、WAF及SEG模組活動的每周報告。

TrustCSI™ ATP 解決方案



1. 當用戶瀏覽網頁時，負責鞏固對外網絡的UTM模組會檢查所有傳輸入內的網頁數據。
2. 網絡應用數據會被傳送至WAF模組進行特徵及行為比對偵測。獲確認安全的數據將被送返UTM模組，而已知的具侵害性資訊將被阻截。
3. 電子郵件會被傳送至SEG模組以檢查其內容及附件。網絡及用戶均免受垃圾郵件和惡意軟件侵襲。
4. 未知和可疑的檔案會被傳送至負責病毒檢疫的「沙盒」。整個程序將在模擬及隔離環境內進行。
5. 惡意或可疑的檔案一被識別，沙盒將通知相關模組作自動回應或消除。

TrustCSI™ ATP 進階威脅防護方案的五大安全組件

- **UTM** — **統一威脅管理(UTM)**：高性能的安全閘道能全面防禦複雜的網絡、內容及應用層級威脅。
- **WAF** — **網絡應用防火牆(WAF)**：使用先進的雙向保護技術，抵擋進階的網絡應用威脅如SQL注入攻擊及跨站腳本攻擊。
- **SEG** — **電子郵件安全設備(SEG)**：抵禦各種電郵安全威脅，包括網絡釣魚及惡意程式附件。
- **Sandbox** — **沙盒**：將有嫌疑的檔案放入虛擬機器內運行，從而確認它們的本質及風險水平，並通過與其他安全組件的自動化整合來消除風險。
- **MSS** — **託管式安全服務(MSS)**：提供24 x 7全面預防、偵測、修正、監察及實時警報服務。它能透過安全智能平台分析系統漏洞及辨識真正威脅。

中信國際電訊CPC

W: www.citictel-cpc.com
亞太區: info@citictel-cpc.com
歐洲及CIS: info-eu@citictel-cpc.com

香港 T: 852 2170 7101
日本 T: 81 3 5339 1968
愛沙尼亞 T: 372 622 33 99
俄羅斯 T: 7 495 981 5676
台灣 T: 886 2 6600 2588
馬來西亞 T: 603 2280 1500
波蘭 T: 48 22 630 63 30
荷蘭 T: 31 20 567 2000
中國大陸 (Toll Free): 400 651 7550
新加坡 T: 65 6220 6606

TAP1909TC